UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information under the control of Google LLC and more fully described in Attachment A.	)	Case No. 21-1029M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 12/30/2021 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Nancy Joseph .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 12/16/2021 @ 10:28 a.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property To Be Searched

This warrant is directed to Google LLC and applies to:

(1) location history data, sourced from methods including GPS, wi-fi, and Bluetooth, generated from devices and that reported a device location within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below ("Initial Search Parameters"); and

(2) identifying information for Google Accounts associated with the responsive location history data.

Initial Search Parameters

- Date: December 11, 2021
- Time Period (including time zone): 8:30 PM to 11:00 PM (CST)
- Target Location: Geographical area identified as a rectangle defined by latitude/longitude coordinates connected by straight lines:
  (1) 42.959476, -88.106514; (2) 42.959402, -88.104272; (3) 42.956842, -88.104277; (4) 42.957201, -88.106431.
- Time Restriction: Devices that reported their location as being within the Target Location at 8:30 PM to 11:00 PM (CST) on December 11, 2021.


42.959476,
-88.106514
42.959402,
-88.104272
42.957201,
-88.106431
42.956842,
-88.104277
Target
Target Mobile
CardInnvtec ATM
Starbucks
15470 Belgit Rd, New Berlin, WI 53151
Google

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google

Google shall provide responsive data (as described in Attachment A) to the government pursuant to the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A.

2. For each location point recorded within the Initial Search Parameters, Google shall produce to the government anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the "Anonymized List").

3. The government shall review the Anonymized List in order to prioritize the devices about which it wishes to obtain identifying information.

4. Google is required to disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Account associated with each device ID about which the government inquires.

II. Information to Be Seized

All information described above in Section I that constitutes evidence of theft of firearms from a Federal Firearms Licensee (FFL), in violation of Title 18, United States Code, Sections 922(j), 922(u), 924(a)(2), 924(l), and 924(m).

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information under the control of Google LLC and more fully described in Attachment A.

Case No. 21-1029M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Sections 922(j), 922 (u), 924(a)(2), 924(1), & 924 (m)	Theft of firearms from a Federal Firearms Licensee (FFL),

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Anthony Winkler, ATF Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 12/16/2021

Judge's signature

City and state: Milwaukee, WI

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, **Anthony Winkler**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachments A and B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been since March 2016. As an ATF Special Agent, I have participated in numerous investigations regarding the unlawful possession of firearms by convicted felons. I have also conducted investigations related to the unlawful use of firearms, firearms trafficking, drug trafficking, and arson.

3. Prior to my employment with ATF, I was a Uniform Division Officer with the United States Secret Service (USSS) for nearly 11 years. My duties included providing physical security for both the Vice President's Residence as well as the White House. Other duties included planning and implementing Counter Sniper protection protocols for Presidential and Vice Presidential travel, both foreign and domestic.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe unknown persons committed knowingly stole firearms from a Federal Firearms Licensee (FFL), in violation of Title 18, United States Code, Sections 922(j), 922(u), 924(a)(2), 924(l), and 924(m). There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Eastern District of Wisconsin is "a district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

7. Based on my training and experience, I know that cellular devices, such as mobile telephone(s), are wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. In order to send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called "cell sites," which can be mounted on towers, buildings, or other infrastructure. Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers. As a result, information about what cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device at that point.

8. Based on my training and experience, I also know that many cellular devices such as mobile telephones have the capability to connect to wireless Internet ("wi-fi") access points if a user enables wi-fi connectivity. Wi-fi access points, such as those created through the use of a

router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

9. Based on my training and experience, I also know that many cellular devices feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by mobile devices within the Bluetooth device's transmission range, to which it might connect.

10. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the phone can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the app's operation.

11. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

12. In addition, based on my training and experience, I know that Google offers numerous online-based services, including email (Gmail), navigation (Google Maps), search

engine (Google), online file storage (including Google Drive, Google Photos, and YouTube), messaging (Google Hangouts and Google Allo), and video calling (Google Duo). Some services, such as Gmail, online file storage, and messaging, require the user to sign in to the service using their Google account. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address. Other services, such as Google Maps and YouTube, can be used while signed into a Google account, although some aspects of these services can be used even without being signed into a Google account.

13. In addition, based on my training and experience, I know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign into a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be synced across the various devices on which they may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices.

14. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

15. Based on my training and experience, I know that Google collects and retains location data from devices running the Android operating system when the user has enabled Google location services. Google then uses this information for various purposes, including to

tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. In addition, I know that Google collects and retains data from non-Android devices that run Google apps if the user has enabled location sharing with Google. Google typically associates the collected location information with the Google account associated with the Android device and/or that is signed in via the relevant Google app. The location information collected by Google is derived from sources including GPS data, information about the cell sites within range of the mobile device, and information about wi-fi access points and Bluetooth beacons within range of the mobile device.

16. Based on my training and experience, I also known that Google collects and retains information about the user's location if the user has enabled Google to track web and app activity. According to Google, when this setting is enabled, Google saves information including the user's location and Internet Protocol address at the time they engage in certain Internet- and app- based activity and associates this information with the Google account associated with the Android device and/or that is signed in with the relevant Google app.

17. Location data, such as the location data in the possession of Google, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected via the use of Google products as described above, mobile devices that were in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can inculpate or exculpate a Google account holder by showing that he was, or was not, near a given location at a time relevant to the criminal investigation.

18. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

19. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

PROBABLE CAUSE

20. On December 11, 2021, a burglary took place at Dunham's Sports, a FFL located at 15470 W. Beloit Rd, New Berlin, Wisconsin, in the Eastern District of Wisconsin. An

unknown group of five individuals entered Dunham's at approximately 9:00 pm and proceeded to the firearms section of the store. Based on surveillance video from inside Dunham's, one of the individuals from the group of five hid in a floor display until after the store was closed and locked by employees. The last employee departed Dunham's around 10:25 pm. Approximately 15 minutes after the last employee left Dunham's, an unknown individual wearing a mask emerged from their hiding place and proceeded to break into the pistol display case.

21. An alarm was triggered by the unknown individual which led officers from the New Berlin Police Department to respond to Dunham's. The employee with the keys to the store arrived at approximately 11:44 pm to allow Officers to check the alarm. Upon inspection, it was discovered that 18 pistols were stolen from the glass display case.

22. Based on surveillance video and photos, the individual who was captured standing on the glass display case at 10:38 pm, can be seen using his/her cellular telephone in the store at 9:01 pm.

23. Based on the foregoing, I submit that there is probable cause to search information in the possession of Google relating to what devices were in the Target Location described in Attachment A during the time period described in Attachment A, as well as information that identifies the Google accounts with which those devices are associated, for evidence of the crime(s) at issue in this case. Among other things, this information can inculpate or exculpate a Google account holder by showing that he was, or was not, near a given location at a time relevant to the criminal investigation.

24. In order to facilitate the manageable disclosure of and search of this information, the proposed warrant contemplates that Google will disclose the information to the government

in stages rather than disclose all of the information for which the government has established probable cause to search at once. Specifically, as described in Attachment B.I:

a. Google will be required to disclose to the government an anonymized list of devices that specifies information including the corresponding unique device ID, timestamp, coordinates, and data source, if available, of the devices that reported their location within the Target Location described in Attachment A during the time period described in Attachment A.

b. The government will then review this list in order to prioritize the devices about which it wishes to obtain associated information.

c. Google will then be required to disclose to the government the information identifying the Google account(s) for those devices about which the government further inquires.

CONCLUSION

25. Based on the forgoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c).

26. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

1. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

ATTACHMENT A

Property To Be Searched

This warrant is directed to Google LLC and applies to:

(1) location history data, sourced from methods including GPS, wi-fi, and Bluetooth, generated from devices and that reported a device location within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below ("Initial Search Parameters"); and

(2) identifying information for Google Accounts associated with the responsive location history data.

Initial Search Parameters

- Date: December 11, 2021
- Time Period (including time zone): 8:30 PM to 11:00 PM (CST)
- Target Location: Geographical area identified as a rectangle defined by latitude/longitude coordinates connected by straight lines:
  (1) 42.959476, -88.106514; (2) 42.959402, -88.104272; (3) 42.956842, -88.104277; (4) 42.957201, -88.106431.
- Time Restriction: Devices that reported their location as being within the Target Location at 8:30 PM to 11:00 PM (CST) on December 11, 2021.


42.959476,
-88.106514
42.959402,
-88.104272
42.957201,
-88.106431
42.956842,
-88.104277
Target
Target Mobile
CardInvites ATM
Starbucks
Michaels
15470 Belgot Rd, New Berlin, WI 53151
Hair Solutions Salon & Spa
Buffalo Wild Wings
Google

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google

Google shall provide responsive data (as described in Attachment A) to the government pursuant to the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A.

2. For each location point recorded within the Initial Search Parameters, Google shall produce to the government anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the "Anonymized List").

3. The government shall review the Anonymized List in order to prioritize the devices about which it wishes to obtain identifying information.

4. Google is required to disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Account associated with each device ID about which the government inquires.

II. Information to Be Seized

All information described above in Section I that constitutes evidence of theft of firearms from a Federal Firearms Licensee (FFL), in violation of Title 18, United States Code, Sections 922(j), 922(u), 924(a)(2), 924(l), and 924(m).

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ electronic records and electronic spreadsheets I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature